

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001

REMARKS

Applicants appreciate the Examiner's thorough examination of the present application. By this amendment, the specification is again being amended to delete the hyperlinks as requested by the Examiner. Also, dependent Claim 25 is again being amended to correct a minor informality as helpfully pointed out, the Examiner. The independent Claims 21, 31 and 44 are amended to further clarify the present invention.

The patentability of the claims is discussed in greater detail below. Favorable reconsideration is respectfully requested.

I. The Claimed Invention

Independent Claim 31, for example, is directed to a device for converting data between an unencrypted format and an encrypted format. The device comprises a register for storing the data in the form of bit words, and a circuit. The circuit is for performing a plurality of transformation rounds, with each transformation round comprising applying at least one transformation to a two-dimensional array of rows and columns of bit words defining a state array. Each transformation round further comprises transposing each of the rows and columns of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array. Independent Claim 21 is a method counterpart to Claim 31 and recites similar recitations. Independent Claim 44 is similar to Claim 31, but further recites that each

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001

transformation round also comprises applying at least one round key to the state array in at least one of the transformation rounds.

II. All The Claims Are Patentable

The Examiner again rejected independent Claims 21, 31, and 44 as being unpatentable over the Ohkuma et al. patent publication for the reasons set forth on pages 4-7 of the Office Action. Applicants contend that independent Claims 21, 31 and 44, and their respective dependent claims, clearly define over the cited reference, and in view of the following remarks, favorable reconsideration of the rejection under 35 U.S.C. §103 is requested.

Each of the independent claims includes transposing each of the rows and columns of the state array to form a transposed state array for at least one of the transformation rounds so that at least one transformation is applied to the transposed state array. It is this combinations of features which is not fairly taught or suggested in the cited reference and which patentably defines over the cited reference.

The Examiner correctly notes that the Ohkuma et al. reference discloses an encryption device. However, the Examiner has continued to mischaracterize the actual teachings of the reference with respect to the higher level MDS (Maximum Distance Separable) matrix. Indeed, the Examiner incorrectly contends (section 4.2 of the final Office Action) that the Ohkuma et al. patent publication discloses "transposing row and columns of the state array to form a higher level matrix that meets the recitation of a transposed state array".

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001

As support for this contention, the Examiner points to paragraphs [0268]-[0273] of the Ohkuma et al. patent publication. Yet paragraph [0268] merely states that a matrix may be obtained by substituting rows, substituting columns, and arbitrarily transposing in an arbitrary MDS matrix. There is nothing in any of the cited paragraphs specifically relied upon by the Examiner that discloses or suggests transposing rows and columns of a state array. It appears that the Examiner is relying upon the Ohkuma et al. reference merely for the use of the term "transposing" included therein.

Additionally, Applicants have amended the independent claims to recite transposing each of the rows and columns of the state array to form a transposed state array. Such an amendment should aid the Examiner in understanding that the phrase "arbitrarily transposing" in the reference cannot be fairly interpreted to meet the features of the invention as claimed. In other words, in Ohkuma et al., there is clearly no transposing of each of the rows and columns of the state array to form a transposed state array. Indeed, it is Applicants who invented this feature, as claimed.

Moreover, as further evidence of the Examiner's failure to present a prima facie case of obviousness, Applicants point to the Examiner's statement on page 5, lines 5-10 of the office action, reproduced below.

Although Ohkuma et al. does not disclose the same architecture as in applicant's disclosure, Ohkuma et al. discloses different arrangements in the disclosure that read on [sic] the claimed language as claimed and any combination or omission of some of the components of exemplified arrangement or any other arrangement disclosed in Ohkuma et al's

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001

would require routine skill in the art and therefore, would be an obvious modification to one skilled in the art to reach a design goal. (emphasis added).

The Examiner's statement amounts to a general allegation that any modification of the Ohkuma et al. system to meet the features of the claimed invention would be obvious. However, a statement that modifications of the prior art to meet the claimed invention would have been within the ordinary skill of the art at the time the claimed invention was made, by itself, is not sufficient to establish a prima facie case of obviousness without some objective reason to modify the teachings of the reference.

As the Examiner is aware, to establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the reference itself or in the knowledge generally available to one of ordinary skill in the art, to modify the reference. Second, there must be a reasonable expectation of success. Finally, the prior art reference must teach or suggest all the claim features. The initial burden is on the Examiner to provide some suggestion of the desirability of doing what the Applicants have done. To support the conclusion that the claimed invention is directed to obvious subject matter, either the reference must expressly or impliedly suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the reference. Both the suggestion to make the claimed combination and the reasonable expectation of success

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001

must be founded in the prior art and not in Applicants' disclosure.

There is simply no teaching or suggestion in the cited reference to provide the combination of features as claimed. Accordingly, for at least the reasons given above, Applicants maintain that the cited reference does not disclose or fairly suggests the invention as set forth in Claims 21, 31 and 44. Furthermore, no proper modification of the teachings of this reference could result in the invention as claimed. Thus, the rejection under 35 U.S.C. §103(a) should be withdrawn.

It is submitted that the independent claims are patentable over the prior art. In view of the patentability of the independent claims, it is submitted that their dependent claims, which recite yet further distinguishing features are also patentable over the cited references for at least the reasons set forth above. Accordingly, these dependent claims require no further discussion herein.


III. Conclusion

In view of the foregoing remarks, it is respectfully submitted that the present application is in condition for allowance. An early notice thereof is earnestly solicited. If, after reviewing this Response, there are any remaining informalities which need to be resolved before the application can be passed to issue, the Examiner is invited and

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 09/974,705
Filed: OCTOBER 10, 2001

respectfully requested to contact the undersigned by telephone
to resolve such informalities.

Respectfully submitted,



PAUL J. DITMYER
Reg. No. 40,455
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
Attorney for Applicants

CERTIFICATE OF FACSIMILE TRANSMISSION

I HEREBY CERTIFY that the foregoing correspondence has
been forwarded via facsimile number 571-273-8300 to the
Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-
1450 this 17th day of February, 2006.